UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with a certain cellular telephone assigned call number (414) 388-7066 that is stored at premises controlled by T-Mobile.

Case No. 21 MJ 156

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2119(1) and 924 (c)	Motor vehicle robbery and use of a firearm during a crime of violence.

The application is based on these facts:

See Attachments.

- ☐ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

BRADLEY KURTZWEIL
Digitally signed by BRADLEY KURTZWEIL
Date: 2021.07.28 09:41:12 -05'00'

Applicant's signature

ATF Special Agent Bradley Kurtzweil

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: July 28, 2021

William E. Duffin

Judge's signature

City and state: Milwaukee, Wisconsin

Hon. William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Bradley Kurtzweil, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (414) 388-7066 that is stored at premises controlled by T-Mobile, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require this same provider to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Special Agent of the United States Justice Department, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), currently assigned to the Milwaukee Field Office. I have been so employed since March 2020. My duties as a Special Agent with ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes.

3. I have completed approximately 26 weeks of training (approximately 1000 hours) at the Federal Law Enforcement Training Center (Glynco, Georgia), as well as the ATF National Academy. That training included various legal courses related to Constitutional Law as well as search and seizure authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as: interviewing, surveillance, and evidence collection.

4. Prior to my employment with the ATF, I was a sworn Police Officer in the State of Illinois from March 2011 to March 2020. I completed 12 Weeks (approximately 480 hours) of basic training at the Illinois State Police Academy from April 2011 to June 2011.

5. My most recent position as a Police Officer, prior to my employment with ATF, was with the Bolingbrook Police Department in Bolingbrook, IL. While employed by the Bolingbrook Police Department, I was a Patrol Officer from December 2012 until March 2020. From July 2017 until March 2020, I also served as an Evidence Technician, assigned to Patrol. During my time in Bolingbrook, I received eight Written Recognitions and two Commendations.

6. During my career as a Police Officer, I attended approximately 520 hours of additional training in areas including: evidence collection, interview/interrogation, arson and explosives, gang investigations; and drug investigations.

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of motor vehicle robbery and use of a firearm during a crime of violence, in violation of Title 18, United States Code, Sections 2119(1) and 924(c).

PROBABLE CAUSE

9. On February 15, 2021 at approximately 10:19 PM, the Menomonee Falls Police Department received a complaint of an armed robbery in the parking lot of the Delta Marriot Hotel, located at N88 W14750 Main St, Menomonee Falls, Waukesha County, Wisconsin.

10. Upon the arrival of officers, it was discovered that the victim (AV), an employee arriving for work, was pulled out of the driver's side of her parked vehicle as a gun was held to her head by Offender 1. AV reported being pushed on her right shoulder by another subject, Offender 2, who had entered the passenger side door of the vehicle. She reported that Offender 2 shoved her on the shoulder with his hands, yelling at her to get out of the car.

11. AV reported after she was pulled from her vehicle, Offender 1 threw her phone at AV while she was lying on the ground. The phone landed behind the rear driver side tire, causing AV to fear the phone would be run over by her vehicle as it drove in reverse. As AV retrieved her phone, Offender 1 again pointed the gun at her head and demanded her car keys stating, "Give me your keys or I'll shoot." After giving Offender 1 her keys, he stated, "Too slow," and took AV's cellphone from her, before getting back into the driver side of the car. Offender 2 exited the vehicle and told AV, "Gimme your cash bitch," at which time AV complied with his demand. After having her car keys, cell phone and U.S. currency taken from her, she got off the ground and ran into the hotel to call 911. The two offenders then fled in AV's vehicle, without her consent.

12. AV's vehicle was located by responding officers on the west end of the hotel parking lot, stuck in the snow approximately 100 yards from the hotel. The doors were left open and the vehicle was unoccupied. AV's cell phone was located by officers in a snowbank in the entrance corner of the parking lot to the Focus Credit Union, which is the first building directly west of the hotel and just across the street from where AV's vehicle was located. Shoe prints in the freshly fallen snow led officers from the hotel parking lot, heading south across Main Street before leaving the sidewalk headed through the property located at N87 W15039 Main St. The shoe prints continued into backyards of the residences located on Rozanne Drive. At this time, a

Washington County Deputy encountered both subjects hiding under a tree in the back yard of W150 N8676 Wheeler Drive, which runs perpendicular to Rozanne Drive and connects at the south end of Rozanne where it dead ends. Deputies took one subject, later identified as Troy Walter, M/B, 10/29/1997, into custody, while the other subject, identified as Delawn McNutt, M/B, 09/16/1996, ran through the yard and was apprehended several seconds later by the Menomonee Falls Police Department. Both subjects matched the description of the offenders given by AV and as seen on surveillance videos.

13. A black Samsung A01 cellphone was recovered by a Germantown Police canine during an article search under the trees where McNutt and Walter were seen hiding.

14. Seven rounds of .22 caliber ammunition were located on McNutt's person during a search incident to his arrest by Menomonee Falls Police Officers.

15. On March 4, 2021, a High Standard, Model DM 101, .22 caliber Derringer was located by ATF Special Agent Jason Salerno and his canine partner Sandi. The firearm was located in the rear yard of N87 W15042 Rozanne Dr. The location where the firearm was located is approximately 20 yards from where McNutt was taken into custody. See Map Below.

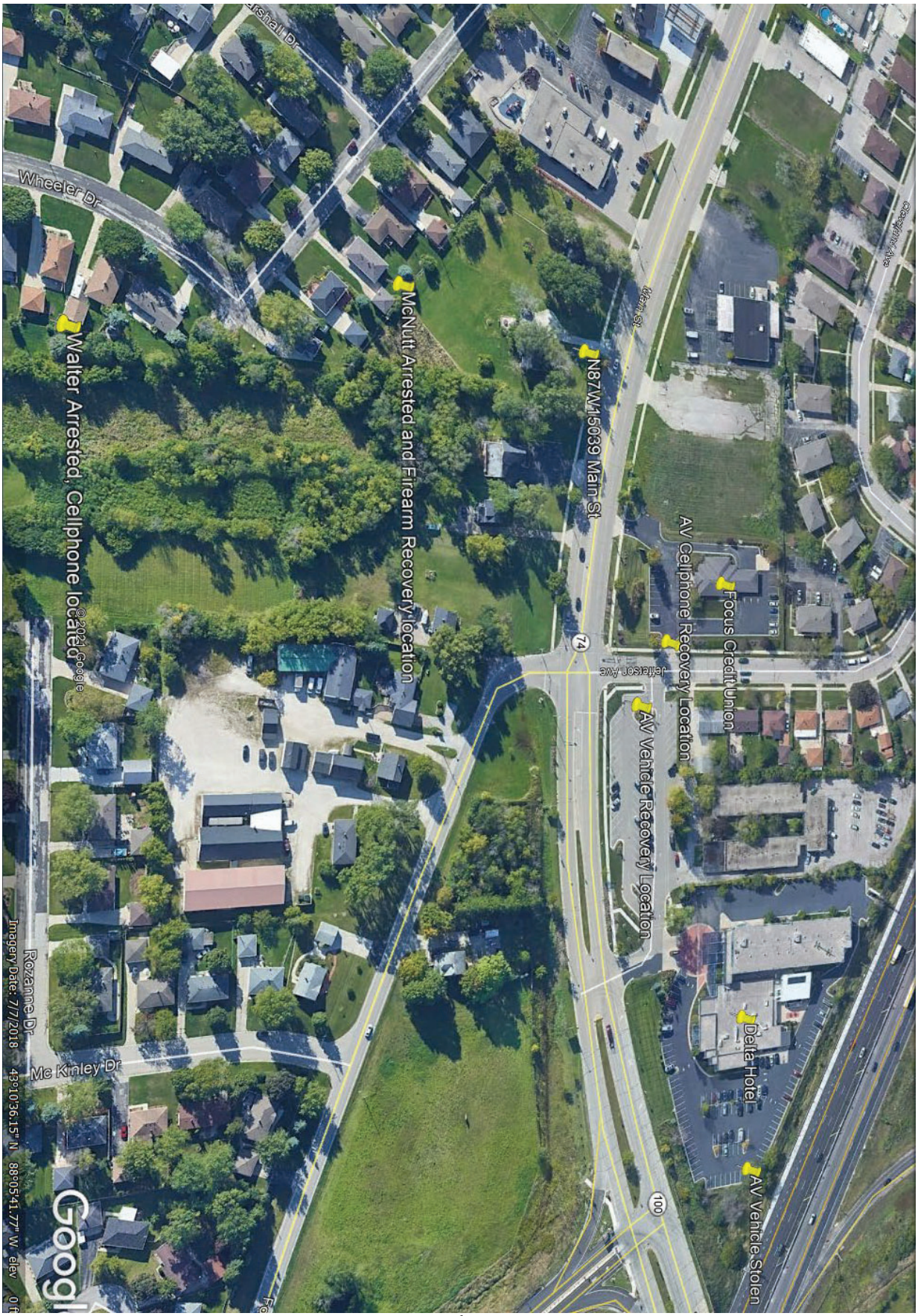
16. Law enforcement has been monitoring the jail phone calls made by McNutt and Walter during the entirety of their imprisonment in the Waukesha County Jail. During these phone calls, both subjects have placed phone calls to a subject whom they refer to as "Meech," at phone number (414-388-7066). During these phone calls, both McNutt and Walter have made statements to "Meech" that they were angry with him for not being caught as well, indicating there was a possible 3rd subject involved in the events during the evening of February 15, 2021. Law enforcement was initially unsuccessful in identifying "Meech," and the role this individual played, if any.

17. On June 30, 2021, the United States Attorney's office received notice from McNutt's attorney of a possible defense alibi witness named Demetrius Jovante Brown (M/B xx/xx/1997), whom they advised had information regarding the case, specifically that McNutt was with him the night of the carjacking and thus McNutt could not have committed the crime. Law enforcement observed the defense report listed a phone number for Brown as "414-388-7066."

18. Law enforcement identified Brown's last known address and attempted to interview Brown, but were unsuccessful in contacting him at his listed residence. However, family members who were home referred to Brown as, "Meech."

19. Having identified "Meech" as Brown, law enforcement reviewed jail phone calls once again. Law enforcement identified a phone call between Walter and Brown, made on February 17, 2021, at approximately 12:22 PM. During the phone call at approximately the 4:46 minute mark, Brown stated to Walter, "Yo bitch ass kept telling me bro to trail y'all bro I should have just trailed y'all bro." Walter responded, "I was like, we told this bitch ass nigga to trail us."

20. Law Enforcement has also reviewed phone records from Walter, Facebook records from both Walter and McNutt, as well as cell site data for both McNutt and Walter. The information obtained pursuant to the previously issued Federal Search Warrants, indicated Walter to be in contact with Brown during the time frame in which the carjacking took place and immediately afterwards.


Wheeler Dr
Walter Arrested, Cellphone located
McNutt Arrested and Firearm Recovery location
N87W15039 Main St
Main St
AV Cellphone Recovery Location
Focus Credit Union
Jefferson Ave
AV Vehicle Recovery Location
Delta Hotel
AV Vehicle Stolen
Rozanne Dr
Mc Kinley Dr
74
100
Imagery Date: 7/7/2018 43°10'36.15" N 88°05'41.77" W elev 0 ft
Google

TECHNICAL INFORMATION

21. Based on my training and experience, I know that cellular telephone providers can collect historical and prospective cell-site data and historical and prospective E-911 Phase II data about the location of the cellular telephones to which they provide service, including by initiating a signal to determine the location of the cellular telephone on cellular telephone provider networks or with such other reference points as may be reasonably available.

22. In my training and experience, I have learned that cellular telephone providers are companies that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone, but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

23. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the

customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication.

24. Based on my training and experience, I know that cellular telephone providers can collect cell-site data about the cellular telephones using its network. I also know that wireless providers typically collect and retain cell-site and other cellular network data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes. From this data, wireless providers can also estimate the historical locations of cellular telephones using their networks. These estimates are drawn from data collected in the normal course of business, including cell-site and other cellular network data.

25. I know that some providers of cellular telephone service, have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. I also know that certain wireless providers can provide precision location information, also known as estimated location records or historical handset location data, on both a historical and prospective basis. Each provider refers to its proprietary estimates of a cellular device's location differently. This information, however, is sometimes referred to as geolocation information (PING), Network Event Location System (NELOS) data, Global Positioning System (GPS) data, cell

tower triangulation or trilateration, round-trip time or real-time tool (RTT), per-call measurement data (PCMD), historical E911 data, or precision measurement information.

26. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identity ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

27. Based on my training and experience, I know that wireless providers typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the methods of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business.

AUTHORIZATION REQUEST

28. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

29. I further request that the Court direct the Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number (414) 388-7066 that is stored at premises controlled by T-Mobile, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to Account), for the time period from February 13, 2021 through February 16, 2021:

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses);

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received, including the locations of any cell tower and antenna face; and

iii. historical location records (including historical locational precision information, historical handset location data, estimated location records, geolocation information (PING), Network Event Location System (NELOS) data, Global Positioning System (GPS) data, cell tower triangulation or trilateration, round-trip time (RTT), per-call measurement data (PCMD), historical E911 data, or precision measurement information).

c. A list of definitions or keys identifying all information contained in the records.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of the federal prohibitions against motor vehicle robbery and use of firearm in a crime of violence, in violation of Title 18, United States Code, Section 2119(1), and in violation of Title 18, United States Code, Section 924(c).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **T-Mobile**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **T-Mobile**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **T-Mobile**, and they were made by **T-Mobile** as a regular practice; and

b. such records were generated by **T-Mobile**'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **T-Mobile** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **T-Mobile**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature